

WHAT IS CLAIMED IS:

1. A method for detecting malicious code patterns in consideration of control and data flows, wherein:

5 a malicious code pattern is detected by determining whether values of tokens (variables or constants) included in two sentences to be examined will be identical to each other during execution of the sentences, and

the determination on whether the values of the tokens will be identical to each other during the execution is made through classification into four cases: a case where
10 both tokens in two sentences are constants, a case where one of tokens of two sentences is a constant and the other token is a variable, a case where both tokens of two sentences are variables and have the same name and range, and a case where both tokens of two sentences are variables but do not have the same name and range.

15 2. The method as claimed in claim 1, wherein the determination on whether the values of tokens will be identical during the execution of the sentences is made based on:

if both the tokens in the two sentences are constants, whether relevant token character strings are identical to each other;

20 if one of the tokens of the two sentences is a constant and the other token is a variable, whether the relevant token character strings are identical to each other after the variable is substituted for a constant;

if both the tokens of the two sentences are variables and have the same name and range, whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof; and

25 if both the tokens of two sentences are variables but do not have the same name and range, whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof after the relevant variables are substituted for original variables.